STIG

- What is STIG?
- Why STIG guidance matters
- How Docker Hardened Images help apply STIG guidance
- Identify images that include STIG scan results
- Use a STIG variant
- View and verify STIG scan results
  - View STIG scan attestations
  - Extract HTML report
  - Extract XCCDF report
  - View STIG scan summary

{{< summary-bar feature_name="Docker Hardened Images" >}}

What is STIG?

Security Technical Implementation Guides (STIGs) are configuration standards published by the U.S. Defense Information Systems Agency (DISA). They define security requirements for operating systems, applications, databases, and other technologies used in U.S. Department of Defense (DoD) environments.

STIGs help ensure that systems are configured securely and consistently to reduce vulnerabilities. They are often based on broader requirements like the DoD's General Purpose Operating System Security Requirements Guide (GPOS SRG).

Why STIG guidance matters

Following STIG guidance is critical for organizations that work with or support U.S. government systems. It demonstrates alignment with DoD security standards and helps:

- Accelerate Authority to Operate (ATO) processes for DoD systems
- Reduce the risk of misconfiguration and exploitable weaknesses
- Simplify audits and reporting through standardized baselines

Even outside of federal environments, STIGs are used by security-conscious organizations as a benchmark for hardened system configurations.

STIGs are derived from broader NIST guidance, particularly NIST Special Publication 800-53, which defines a catalog of security and privacy controls for federal systems. Organizations pursuing compliance with 800-53 or related frameworks (such as FedRAMP) can use STIGs as implementation guides that help meet applicable control requirements.

How Docker Hardened Images help apply STIG guidance

Docker Hardened Images (DHIs) include STIG variants that are scanned against custom STIG-based profiles and include signed STIG scan attestations. These attestations can support audits and compliance reporting.

While Docker Hardened Images are available to all, the STIG variant requires a Docker subscription.

Docker creates custom STIG-based profiles for images based on the GPOS SRG and DoD Container Hardening Process Guide. Because DISA has not published a STIG specifically for containers, these profiles help apply STIG-like guidance to container environments in a consistent, reviewable way and are designed to reduce false positives common in container images.

Identify images that include STIG scan results

Docker Hardened Images that include STIG scan results are labeled as **STIG** in the Docker Hardened Images catalog.

To find DHI repositories with STIG image variants, explore images and:

- Use the **Compliance** filter on the catalog page and select **STIG**
- Look for **STIG** labels on individual image listings

To find a STIG image variant within a repository, go to the **Images** tab in the repository, and find images labeled with **STIG** in the **Compliance** column.

Use a STIG variant

To use a STIG variant, you must mirror the repository and then pull the STIG image from your mirrored repository.

View and verify STIG scan results

Docker provides a signed STIG scan attestation for each STIG-ready image. These attestations include:

- A summary of the scan results, including the number of passed, failed, and not applicable checks
- The name and version of the STIG profile used
- Full output in both HTML and XCCDF (XML) formats

View STIG scan attestations

You can retrieve and inspect a STIG scan attestation using the Docker Scout CLI:

```
$ docker scout attest get \
  --predicate-type https://docker.com/dhi/stig/v0.1 \
  --verify \
  --predicate \
  dhi.io/<image>:<tag>
```

Extract HTML report

To extract and view the human-readable HTML report:

```
$ docker scout attest get dhi.io/<image>:<tag> \
  --predicate-type https://docker.com/dhi/stig/v0.1 \
  --verify \
  --predicate \
```

```
  | jq -r '.[0].output[] | select(.format == "html").content | @base64d' > stig_report.html
```

Extract XCCDF report

To extract the XML (XCCDF) report for integration with other tools:

```
$ docker scout attest get dhi.io/<image>:<tag> \
  --predicate-type https://docker.com/dhi/stig/v0.1 \
  --verify \
  --predicate \
  | jq -r '.[0].output[] | select(.format == "xccdf").content | @base64d' > stig_report.xml
```

View STIG scan summary

To view just the scan summary without the full reports:

```
$ docker scout attest get dhi.io/<image>:<tag> \
  --predicate-type https://docker.com/dhi/stig/v0.1 \
  --verify \
  --predicate \
  | jq -r '.[0] | del(.output)'
```

□□□ #2
□ □□□ □□□ 2026-10-31 19:16:17 UTC
□ □□□ □□□ 2026-10-31 19:16:18 UTC